

Conditional expanding bounds for two-variable functions over finite valuation rings

Le Quang Ham^{*} Pham Van Thang[†] Le Anh Vinh[‡]

Abstract

In this paper, we use methods from spectral graph theory to obtain some results on the sum-product problem over finite valuation rings \mathcal{R} of order q^r which generalize recent results given by Hegyvári and Hennecart (2013). More precisely, we prove that, for related pairs of two-variable functions $f(x, y)$ and $g(x, y)$, if A and B are two sets in \mathcal{R}^* with $|A| = |B| = q^\alpha$, then

$$\max \{|f(A, B)|, |g(A, B)|\} \gtrsim |A|^{1+\Delta(\alpha)},$$

for some $\Delta(\alpha) > 0$.

1 Introduction

Let \mathbb{F}_q be a finite field of q elements where q is a large odd prime power. Let \mathcal{A} be a non-empty subset of a finite field \mathbb{F}_q . We consider the sum set

$$\mathcal{A} + \mathcal{A} := \{a + b : a, b \in \mathcal{A}\}$$

and the product set

$$\mathcal{A} \cdot \mathcal{A} := \{a \cdot b : a, b \in \mathcal{A}\}.$$

Let $|\mathcal{A}|$ denote the cardinality of \mathcal{A} . Bourgain, Katz and Tao ([3]) showed that when $1 \ll |\mathcal{A}| \ll q$ then $\max(|\mathcal{A} + \mathcal{A}|, |\mathcal{A} \cdot \mathcal{A}|) \gtrsim |\mathcal{A}|^{1+\epsilon}$, for some $\epsilon > 0$. This improves the trivial bound $|\mathcal{A} + \mathcal{A}| |\mathcal{A} \cdot \mathcal{A}| \gtrsim |\mathcal{A}|$. (Here, and throughout, $X \lesssim Y$ means that there exists $C > 0$ such that $X \leq CY$, and $X \ll Y$ means that $X = o(Y)$.) The precise statement of their result is as follows.

^{*}University of Science, Vietnam National University Hanoi Email: hamlaoshi@gmail.com

[†]EPFL, Lausanne, Switzerland. Research partially supported by Swiss National Science Foundation Grants 200020-144531 and 200021-137574. Email: thang.pham@epfl.ch

[‡]University of Education, Vietnam National University Hanoi. Research was supported by Vietnam National Foundation for Science and Technology Development grant 101.99-2013.21. Email: vinhla@vnu.edu.vn

Theorem 1.1. ([3, Theorem 1.1]) Let \mathbb{F}_q be a finite field of q elements where q is an odd prime. Let \mathcal{A} be a subset of \mathbb{F}_q such that

$$q^\delta < |\mathcal{A}| < q^{1-\delta}$$

for some $\delta > 0$. Then one has a bound of the form

$$\max \{|\mathcal{A} + \mathcal{A}|, |\mathcal{A} \cdot \mathcal{A}|\} \gtrsim |\mathcal{A}|^{1+\epsilon}$$

for some $\epsilon = \epsilon(\delta) > 0$.

Note that the relationship between ϵ and δ in Theorem 1.1 is difficult to determine. In [15], Hart, Iosevich, and Solymosi obtained a bound that gives an explicit dependence of ϵ on δ . More precisely, if $|A + A| = m$ and $|A \cdot A| = n$, then

$$|A|^3 \leq \frac{cm^2n|A|}{q} + cq^{1/2}mn, \quad (1.1)$$

for some positive constant c . Inequality (1.1) implies a non-trivial sum-product estimate when $q^{1/2} \lesssim |A| \lesssim q$. Using methods from the spectral graph theory, the third listed author [26] improved (1.1) and as a result, obtained a better sum-product estimate.

Theorem 1.2. ([26, Theorem 4]) For any set $A \subseteq \mathbb{F}_q$, if $|A + A| = m$, and $|A \cdot A| = n$, then

$$|A|^2 \leq \frac{mn|A|}{q} + q^{1/2}\sqrt{mn}.$$

Corollary 1.3. ([26, Corollary 2]) For any set $A \subseteq \mathbb{F}_q$, we have If $q^{1/2} \ll |A| < q^{2/3}$, then

$$\max \{|A + A|, |A \cdot A|\} \gtrsim \frac{|A|^2}{q^{1/2}}.$$

If $q^{2/3} \leq |A| \ll q$, then

$$\max \{|A + A|, |A \cdot A|\} \gtrsim (q|A|)^{1/2}.$$

It follows from Corollary 1.3 that if $|A| = p^\alpha$, then

$$\max \{|A + A|, |A \cdot A|\} \gtrsim |A|^{1+\Delta(\alpha)},$$

where $\Delta(\alpha) = \min \{1 - 1/2\alpha, (1/\alpha - 1)/2\}$. In the case that q is a prime, Corollary 1.3 was proved by Garaev [11] using exponential sums. Cilleruelo [9] also proved related results using dense Sidon sets in finite groups involving \mathbb{F}_q and $\mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$ (see [9, Section 3] for more details).

We note that a variant of Corollary 1.3 was considered by Vu [28], and the statement is as follows.

Theorem 1.4. [28, Theorem 1.2] Let P be a non-degenerate polynomial of degree k in $\mathbb{F}_q[x, y]$. Then for any $A \subseteq \mathbb{F}_q$, we have

$$\max \{|A + A|, |P(A)|\} \gtrsim \min \{|A|^{2/3} q^{1/3}, |A|^{3/2} q^{-1/4}\},$$

where a polynomial P is called non-degenerate if P can not be presented as of the form $Q(L(x, y))$ with Q is an one-variable polynomial and L is a linear form in x and y .

It also follows from Theorem 1.4 that if $|A| = p^\alpha$, then

$$\max \{|A + A|, |P(A)|\} \gtrsim |A|^{1+\Delta(\alpha)},$$

where $\Delta(\alpha) = \min(1/2 - 1/4\alpha, (1/\alpha - 1)/3)$.

Recently, Hegyvári and Hennecart [17] obtained analogous results of these problems by using a generalization of Solymosi's approach in [24]. In particular, they proved that for some certain families of two-variable functions $f(x, y)$ and $g(x, y)$, if $|A| = |B| = p^\alpha$, then $\max \{|f(A, B)|, |g(A, B)|\} \gtrsim |A|^{1+\Delta(\alpha)}$, for some $\Delta(\alpha) > 0$. Before giving their first result, we need the following definition on the multiplicity of a function defined over a subgroup over finite fields.

Let G be a subgroup in \mathbb{F}_p^* , and $g: G \rightarrow \mathbb{F}_p$ an arbitrary function, we define

$$\mu(g) = \max_t |\{x \in G: g(x) = t\}|.$$

Theorem 1.5. ([17, Theorem 2.2]) Let G be a subgroup of \mathbb{F}_p^* , and $f(x, y) = g(x)(h(x) + y)$ be defined on $G \times \mathbb{F}_p^*$, where $g, h: G \rightarrow \mathbb{F}_p^*$ are arbitrary functions. Put $m = \mu(g \cdot h)$. For any sets $A \subset G$ and $B, C \subset \mathbb{F}_p^*$, we have

$$|f(A, B)| |B \cdot C| \gtrsim \min \left\{ \frac{|A| |B|^2 |C|}{pm^2}, \frac{p|B|}{m} \right\}.$$

In particular, if $f(x, y) = x(1 + y)$, then, as a consequence of Theorem 1.5, we obtain the following corollary which also studied by Garaev and Shen in [12].

Corollary 1.6. For any set $A \subseteq \mathbb{F}_p \setminus \{0, -1\}$, we have

$$|A \cdot (A + 1)| \gtrsim \min \left\{ \sqrt{p|A|}, |A|^2/\sqrt{p} \right\}.$$

The next result is the additive version of Theorem 1.5.

Theorem 1.7. ([17, Theorem 2.3]) Let G be a subgroup of \mathbb{F}_p^* , and $f(x, y) = g(x)(h(x) + y)$ be defined on $G \times \mathbb{F}_p^*$ where g and h are arbitrary functions from G into \mathbb{F}_p^* . Put $m = \mu(g)$. For any $A \subset G$, $B, C \subset \mathbb{F}_p^*$, we have

$$|f(A, B)| |B + C| \gtrsim \min \left\{ \frac{|A| |B|^2 |C|}{pm^2}, \frac{p|B|}{m} \right\}$$

Note that by letting $C = A$, this implies that

$$\max \{|f(A, B)|, |A + B|\} \gtrsim |A|^{1+\Delta(\alpha)}, \quad |A| = |B| = p^\alpha,$$

where $\Delta(\alpha) = \min \{1 - 1/2\alpha, (1/\alpha - 1)/2\}$. In the case g and h are polynomials, and g is non constant, Theorem 1.4, or its generalization in [14] would lead to a similar statement with a weaker exponent $\Delta(\alpha) = \min \{1/2 - 1/4\alpha, 1/3\alpha - 1/3\}$. We also note that Theorem 6 established by Bukh and Tsimmerman [6] does not cover such a function like in Theorem 1.7.

For any function h and $u \in \mathbb{F}_p$, we define $h_u(x) := h(ux)$. In [17], Hegyvári and Hennecart obtained a generalization of Theorem 1.5 as follows.

Theorem 1.8. ([17, Theorem 2.4]) *Let $f(x, y) = g(x)h(y)(x^k + y^k)$ where $g, h : G \rightarrow \mathbb{F}_p^*$ are functions defined on some subgroup G of \mathbb{F}_p^* . We assume that for any fixed $z \in G$, $g(xz)/g(x)$ and $h(xz)/h(x)$ take $O(1)$ different values when $x \in G$ and that $\max_u \mu(g \cdot h_u \cdot \text{id}) = O(1)$. Then for any $A, B, C \subset G$, one has*

$$|f(A, B)| |A \cdot C| |B \cdot C| \gtrsim \min \left\{ \frac{|A|^2 |B|^2 |C|}{p}, p |A| |B| \right\}.$$

The condition on g and h in the theorem looks unusual. For instance, one can take g and h being monomial functions, or functions of the form $\lambda^{\alpha(x)} x^k$, where $\lambda \in \mathbb{F}_p^*$ has order $O(1)$ and $\alpha(x)$ is an arbitrary function. Note that in some particular cases, we can obtain better results. The following theorem is an example.

Theorem 1.9. ([17]) *Let A, B, C be subsets in \mathbb{F}_p^* , and $f(x, y) = xy(x + y)$ a polynomial in $\mathbb{F}_p[x, y]$. Then we have the following estimate*

$$|f(A, B)| |B \cdot C| \gtrsim \min \left\{ \frac{|A| |B|^2 |C|}{p}, p |B| \right\}.$$

This result is sharp when $|A| = |B| = \Theta(p^\alpha)$ with $2/3 \leq \alpha < 1$ since, for instance, one can take $A = B = C$ being a geometric progression of length p^α , it is easy to see that $|A \cdot A| \lesssim |A|$, and $|f(A, A)| \leq p$. This implies that $|f(A, A)| |A \cdot A| \lesssim p |A|$.

There is a series of papers dealing with similar results on the sum-product problem, for example, see [4, 5, 13, 14, 16, 18, 19, 21, 23, 25].

Let \mathcal{R} be a finite valuation ring of order q^r , where q is an odd prime power. Throughout, \mathcal{R} is assumed to be commutative, and to have an identity. We note that if $r = 1$ then \mathcal{R} is a finite field of q elements, and if q is a prime number then \mathcal{R} is a finite ring of q^r elements. Let us denote the set of units, non-units in \mathcal{R} by $\mathcal{R}^*, \mathcal{R}^0$, respectively.

The main purpose of this paper is to extend aforementioned results to finite valuation rings with simpler proofs by methods from graph theory. Our first result is as follows.

Theorem 1.10. *Let \mathcal{R} be a finite valuation ring of order q^r , G be a subgroup in \mathcal{R}^* and $f(x), g(y)$ be functions defined from G into \mathcal{R}^* . Suppose that $m_1 = \mu(f), m_2 = \mu(g)$. Then for any $A, B \subseteq G$, we have the following estimate*

$$|f(A)^2 + g(B)| |f(A) + g(B)| \gtrsim \min \left\{ \frac{|A|^2 |B|^2}{m_1^2 m_2^4 q^{2r-1}}, \frac{q^r |A|}{m_1 m_2^2} \right\}.$$

The following result is an easy consequence of Theorem 1.10, which is also a generalization of [20, Theorem 1.8].

Corollary 1.11. *For any set A in \mathcal{R} satisfying $|A| \gtrsim q^{r-1/2}$, we have*

$$|A + A^2| \gtrsim \min \left\{ \sqrt{q^r |A|}, \frac{|A|^2}{\sqrt{q^{2r-1}}} \right\}.$$

Our next result is an extension of Theorem 1.5.

Theorem 1.12. *Let \mathcal{R} be a finite valuation ring of order q^r , G be a subgroup of \mathcal{R}^* , and $f(x, y) = g(x)(h(x) + y)$ be defined on $G \times \mathcal{R}^*$, where $g, h: G \rightarrow \mathcal{R}^*$ are arbitrary functions. Put $m = \mu(g \cdot h)$. For any sets $A \subset G$ and $B, C \subset \mathcal{R}^*$, we have*

$$|f(A, B)| |B \cdot C| \gtrsim \min \left\{ \frac{q^r |B|}{m}, \frac{|A| |B|^2 |C|}{m^2 q^{2r-1}} \right\}.$$

In the case, $f(x, y) = x(1 + y)$, we obtain the following estimate which generalizes Theorem 1.3 and Theorem 1.4 in [20].

Corollary 1.13. *For any set $A \subset \mathcal{R} \setminus \{\mathcal{R}^0, \mathcal{R}^0 - 1\}$, we have*

$$|A(A + 1)| \gtrsim \min \left\{ \sqrt{q^r |A|}, \frac{|A|^2}{\sqrt{q^{2r-1}}} \right\}.$$

As in Theorem 1.7, we obtain the additive version of Theorem 1.12 as follows.

Theorem 1.14. *Let \mathcal{R} be a finite valuation ring of order q^r , G be a subgroup of \mathcal{R}^* , and $f(x, y) = g(x)(h(x) + y)$ be defined on $G \times \mathcal{R}^*$ where g and h are arbitrary functions from G into \mathcal{R}^* . Put $m = \mu(g)$. For any $A \subset G$, $B, C \subset \mathcal{R}^*$, we have*

$$|f(A, B)| |B + C| \gtrsim \min \left\{ \frac{q^r |B|}{m}, \frac{|A| |B|^2 |C|}{m^2 q^{2r-1}} \right\}.$$

Combining Theorem 1.12 and Theorem 1.14, we obtain the following corollary.

Corollary 1.15. *Let $f(x, y) = g(x)(x + y)$ such that $\mu(g) = O(1)$, and $A \subset \mathcal{R}^*$. Then*

$$|f(A, A)| \times \min \{|A \cdot A|, |A + A|\} \gtrsim \min \left\{ q^r |B|, \frac{|A| |B|^2 |C|}{q^{2r-1}} \right\}.$$

Finally, we will derive generalizations of Theorem 1.8 and Theorem 1.9.

Theorem 1.16. *Let \mathcal{R} be a finite valuation ring of order q^r , and $f(x, y) = g(x)h(y)(x + y)$ where $g, h: G \rightarrow \mathcal{R}^*$ are functions defined on some subgroup G of \mathcal{R}^* . We assume that for any fixed $z \in G$, $g(xz)/g(x)$ and $h(xz)/h(x)$ take $O(1)$ different values when $x \in G$ and that $\max_u \mu(g \cdot h_u \cdot \text{id}) = O(1)$. Then for any $A, B, C \subset G$, one has*

$$|f(A, B)| |A \cdot C| |B \cdot C| \gtrsim \min \left\{ q^r |A| |B|, \frac{|A|^2 |B|^2 |C|}{q^{2r-1}} \right\}.$$

Similarly, we can improve Theorem 1.16 for some special cases of $f(x, y)$. The following theorem is an example, which is also viewed as an extension of Theorem 1.9.

Theorem 1.17. *Let \mathcal{R} be a finite valuation ring of order q^r , and A, B, C be subsets in \mathcal{R}^* , $f(x, y) = xy(g(x) + y)$, where g is a function from \mathcal{R}^* into \mathcal{R}^* , and $\mu(g^2 \cdot id) = O(1)$. Then we have*

$$|f(A, B)| |B \cdot C| \gtrsim \min \left\{ q^r |B|, \frac{|A| |B|^2 |C|}{q^{2r-1}} \right\}.$$

Note that we also can obtain similar results over \mathbb{Z}_m by using Lemma 4.1 in [27] instead of Lemma 3.2.

The rest of this paper is organized as follows. In section 2, we give the definition and some properties of finite valuation rings. In section 3, we mention some properties of pseudo-random graphs. The proof of Theorem 1.10 is given in Section 4, the proofs of Theorems 1.12 and 1.14 are given in Section 5, and the proofs of Theorems 1.16 and 1.17 are given in Section 6.

2 Preliminaries

We start this section by recalling the definition of finite valuation rings.

Definition 2.1. *Finite valuation rings are finite rings that are local and principal.*

Throughout, rings are assumed to be commutative, and to have an identity. Let \mathcal{R} be a finite valuation ring, then \mathcal{R} has a unique maximal ideal that contains every proper ideals of \mathcal{R} , which implies that there exists a non-unit z called *uniformizer* in \mathcal{R} such that the maximal ideal is generated by z . Moreover, we also note that the uniformizer z is defined up to a unit of \mathcal{R} .

There are two structural parameters associated to \mathcal{R} as follows: the cardinality of the residue field $F = \mathcal{R}/(z)$, and the nilpotency degree of z , where the nilpotency degree of z is the smallest integer r such that $z^r = 0$. Let us denote the cardinality of F by q . In this note, q is assumed to be odd, then 2 is a unit in \mathcal{R} .

If \mathcal{R} is a finite valuation ring, and r is the nilpotency degree of z , then we have a natural valuation

$$\nu: \mathcal{R} \rightarrow \{0, 1, \dots, r\}$$

defined as follows: $\nu(0) = r$, for $x \neq 0$, $\nu(x) = k$ if $x \in (z^k) \setminus (z^{k+1})$. We also note that $\nu(x) = k$ if and only if $x = uz^k$ for some unit u in \mathcal{R} . Each abelian group $(z^k)/(z^{k+1})$ is a one-dimensional linear space over the residue field $F = \mathcal{R}/(z)$, thus its size is q . This implies that $|(z^k)| = q^{r-k}$, $k = 0, 1, \dots, r$. In particular, $|(z)| = q^{r-1}$, $|\mathcal{R}| = q^r$ and $|\mathcal{R}^*| = |\mathcal{R}| - |(z)| = q^r - q^{r-1}$, (for more details about valuation rings, see [2], [8], [10], and [22]). The following are some examples of finite valuation rings:

1. Finite fields \mathbb{F}_q , $q = p^n$ for some $n > 0$.
2. Finite rings \mathbb{Z}_{p^r} , where p is a prime

3. $\mathcal{O}/(p^r)$ where \mathcal{O} is the ring of integers in a number field and $p \in \mathcal{O}$ is a prime.
4. $\mathbb{F}_q[x]/(f^r)$, where $f \in \mathbb{F}_q[x]$ is an irreducible polynomial.

3 Properties of pseudo-random graphs

For a graph G of order n , let $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n$ be the eigenvalues of its adjacency matrix. The quantity $\lambda(G) = \max\{\lambda_2, -\lambda_n\}$ is called the second eigenvalue of G . A graph $G = (V, E)$ is called an (n, d, λ) -graph if it is d -regular, has n vertices, and the second eigenvalue of G is at most λ . Since G is a d -regular graph, d is an eigenvalue of its adjacency matrix with the all-one eigenvector $\mathbf{1}$. If the graph G is connected, the eigenvalue d has multiplicity one. Furthermore, if G is not bipartite, for any other eigenvalue θ of G , we have $|\theta| < d$. Let \mathbf{v}_θ denote the corresponding eigenvector of θ . We will make use of the trick that $\mathbf{v}_\theta \in \mathbf{1}^\perp$, so $J\mathbf{v}_\theta = 0$ where J is the all-one matrix of size $n \times n$ (see [7] for more background on spectral graph theory).

It is well known (see [1, Chapter 9] for more details) that if λ is much smaller than the degree d , then G has certain random-like properties. For two (not necessarily) disjoint subsets of vertices $U, W \subset V$, let $e(U, W)$ be the number of ordered pairs (u, w) such that $u \in U$, $w \in W$, and (u, w) is an edge of G . We recall the following well-known fact (see, for example, [1]).

Lemma 3.1. ([1, Corollary 9.2.5]) *Let $G = (V, E)$ be an (n, d, λ) -graph. For any two sets $B, C \subset V$, we have*

$$\left| e(B, C) - \frac{d|B||C|}{n} \right| \leq \lambda \sqrt{|B||C|}.$$

3.1 Sum-product graphs over finite valuation rings

For any $\lambda \in \mathcal{R}$, the sum-product graph $\mathcal{SP}_{\mathcal{R}}(\lambda)$ is defined as follows. The vertex set of the sum-product graph $\mathcal{SP}_{\mathcal{R}}(\lambda)$ is the set $V(\mathcal{SP}_{\mathcal{R}}(\lambda)) = \mathcal{R} \times \mathcal{R}$. Two vertices $U = (a, b)$ and $V = (c, d) \in V(\mathcal{SP}_{\mathcal{R}}(\lambda))$ are connected by an edge, $(U, V) \in E(\mathcal{SP}_{\mathcal{R}}(\lambda))$, if and only if $a + c + \lambda = bd$. Our construction is similar to that of Solymosi in [24].

Lemma 3.2. *For any $\lambda \in \mathcal{R}$, the sum-product graph, $\mathcal{SP}_{\mathcal{R}}(\lambda)$, is a*

$$\left(q^{2r}, q^r, \sqrt{2rq^{2r-1}} \right) - \text{graph}.$$

Proof. It is easy to see that $\mathcal{SP}_{\mathcal{R}}(\lambda)$ is a regular graph of order q^{2r} and valency q^r . We now compute the eigenvalues of this multigraph. For any two vertices $(a, b), (c, d) \in \mathcal{R} \times \mathcal{R}$, we count the number of solutions of the following system

$$a + u + \lambda = bv, \quad c + u + \lambda = dv, \quad (u, v) \in \mathcal{R} \times \mathcal{R}. \quad (3.1)$$

For each solution v of

$$(b - d)v = a - c, \quad (3.2)$$

there exists a unique u satisfying the system (3.1). Therefore, we only need to count the number of solutions of (3.2). Suppose that $\nu(b-d) = \alpha$. If $\nu(a-c) < \alpha$, then Eq. (3.2) has no solution. Thus we assume that $\nu(a-c) \geq \alpha$. It follows from the definition of the function ν that there exist u_1, u_2 in \mathcal{R}^* such that $a-c = u_1 z^{\nu(a-c)}$, $b-d = u_2 z^{\nu(b-d)}$. Let $\mu = u_1 z^{\nu(a-c)-\alpha}$ and $x = u_2 z^{\nu(b-d)-\alpha}$. The number of solutions of (3.2) equals the number of solutions $v \in \mathcal{R}$ satisfying

$$x \cdot v - \mu \in (z^{r-\alpha}). \quad (3.3)$$

Since $\nu(b-d) = \alpha$, $x \in \mathcal{R}^*$, and the equation

$$xv - \mu = t$$

has a unique solution for each $t \in (z^{r-\alpha})$. Since $|(z^{r-\alpha})| = q^\alpha$, the number solutions of (3.3) is q^α if $\nu(a-c) \geq \alpha$.

Therefore, for any two vertices $U = (a, b)$ and $V = (c, d) \in V(\mathcal{SP}_{\mathcal{R}}(\lambda))$, U and V have q^α common neighbors if $\nu(b-d) = \alpha$ and $\nu(a-c) \geq \alpha$ and no common neighbor if $\nu(b-d) = \alpha$ and $\nu(c-a) < \alpha$. Let A be the adjacency matrix of $\mathcal{SP}_{\mathcal{R}}(\lambda)$. For any two vertices U, V then $(A^2)_{U,V}$ is the number of common vertices of U and V . It follows that

$$A^2 = J + (q^r - 1)I - \sum_{\alpha=0}^r E_\alpha + \sum_{\alpha=1}^{r-1} (q^\alpha - 1)F_\alpha, \quad (3.4)$$

where:

- J is the all-one matrix and I is the identity matrix.
- E_α is the adjacency matrix of the graph $B_{E,\alpha}$, where for any two vertices $U = (a, b)$ and $V = (c, d) \in V(\mathcal{SP}_{\mathcal{R}}(\lambda))$, (U, V) is an edge of $B_{E,\alpha}$ if and only if $\nu(b-d) = \alpha$ and $\nu(a-c) < \alpha$
- F_α is the adjacency matrix of the graph $B_{F,\alpha}$, where for any two vertices $U = (a, b)$ and $V = (c, d) \in V(\mathcal{SP}_{\mathcal{R}}(\lambda))$, (U, V) is an edge of $B_{F,\alpha}$ if and only if $\nu(b-d) = \alpha$ and $\nu(a-c) \geq \alpha$

For any $\alpha > 0$, we have $|(z^\alpha)| = q^{r-\alpha}$, thus $B_{E,\alpha}$ is a regular graph of valency less than $q^{2r-\alpha}$ and $B_{F,\alpha}$ is a regular graph of valency less than $q^{2(r-\alpha)}$. Since eigenvalues of a regular graph are bounded by its valency, all eigenvalues of E_α are at most $q^{2r-\alpha}$ and all eigenvalues of F_α are at most $q^{2(r-\alpha)}$. Note that E_0 is a zero matrix.

Since $\mathcal{SP}_{\mathcal{R}}(\lambda)$ is a q^r -regular graph, q^r is an eigenvalue of A with the all-one eigenvector $\mathbf{1}$. The graph $\mathcal{SP}_{\mathcal{R}}(\lambda)$ is connected therefore the eigenvalue q^r has multiplicity one. Since the graph $\mathcal{SP}_{\mathcal{R}}(\lambda)$ contains (many) triangles, it is not bipartite. Hence, for any other eigenvalue θ , $|\theta| < q^r$. Let \mathbf{v}_θ denote the corresponding eigenvector of θ . Note that $\mathbf{v}_\theta \in \mathbf{1}^\perp$, so $J\mathbf{v}_\theta = 0$. It follows from (3.4) that

$$(\theta^2 - q^r + 1)\mathbf{v}_\theta = \left(\sum_{\alpha=1}^r E_\alpha - \sum_{\alpha=1}^{r-1} (q^\alpha - 1)F_\alpha \right) \mathbf{v}_\theta.$$

Hence, \mathbf{v}_θ is also an eigenvalue of

$$\sum_{\alpha=1}^r E_\alpha - \sum_{\alpha=1}^{r-1} (q^\alpha - 1) F_\alpha$$

Since absolute value of eigenvalues of sum of matrices are bounded by sum of largest absolute values of eigenvalues of summands. We have

$$\begin{aligned} \theta^2 &\leq q^r - 1 + \sum_{\alpha=1}^r q^{2r-\alpha} + \sum_{\alpha=1}^{r-1} (q^\alpha - 1) q^{2(r-\alpha)} \\ &< 2rq^{2r-1}. \end{aligned}$$

The lemma follows. \square

3.2 Sum-square graphs over finite valuation rings

We define the sum-square graph $\mathcal{SS}_\mathcal{R}$ as follows. The vertex set of the sum-square graph $\mathcal{SS}_\mathcal{R}$ is the set $V(\mathcal{SS}_\mathcal{R}) = \mathcal{R} \times \mathcal{R}$. Two vertices (a, b) and (c, d) in $V(\mathcal{SS}_\mathcal{R})$ are connected by an edge in $E(\mathcal{SS}_\mathcal{R})$ if and only if $a + c = (b + d)^2$. We have the following pseudo-randomness of the sum-square graph $\mathcal{SS}_\mathcal{R}$.

Lemma 3.3. *The sum-square graph $\mathcal{SS}_\mathcal{R}$ is a $(q^{2r}, q^r, \sqrt{2rq^{2r-1}})$ -graph.*

Proof. It is easy to see that $\mathcal{SS}_\mathcal{R}$ is a regular graph of order q^{2r} and valency q^r . We now compute the eigenvalues of this multi-graph. For any two vertices (a, b) and (c, d) , we count the number of solutions of the following system

$$a + u = (b + v)^2, \quad c + u = (d + v)^2, \quad (u, v) \in \mathcal{R} \times \mathcal{R}. \quad (3.5)$$

For each solution v of

$$(b - d)(2v + b + d) = a - c, \quad (3.6)$$

there exists a unique u satisfying the system (3.5). Therefore, we need only count the number of solutions of (3.6). Suppose that $\nu(b - d) = \alpha$. If $\nu(a - c) < \alpha$, then Eq. (3.5) has no solution. Thus we assume that $\nu(a - c) \geq \alpha$. It follows from the definition of the function ν that there exist u_1, u_2 in \mathcal{R}^* such that $a - c = u_1 z^{\nu(a-c)}$ and $b - d = u_2 z^{\nu(b-d)}$. Let $\mu = u_1 z^{\nu(a-c)-\alpha}$ and $x = u_2 z^{\nu(b-d)-\alpha}$. The number of solutions of (3.6) equals the number of solutions $v \in \mathcal{R}$ satisfying

$$x \cdot (2v + b + d) - \mu \in (z^{r-\alpha}). \quad (3.7)$$

Since $\nu(b - d) = \alpha$, we have $x \in \mathcal{R}^*$. So for any $t \in (z^{r-\alpha})$, the equation $x(2v + b + d) - \mu = t$ has a unique solution. Since $|(z^{r-\alpha})| = q^\alpha$, the number solutions of (3.7) is q^α if $\nu(a - c) \geq \alpha$.

Therefore, for any two vertices $U = (a, b)$ and $V = (c, d) \in V(\mathcal{SS}_{\mathcal{R}})$. If $\nu(b - d) = \alpha$ and $\nu(a - c) \geq \alpha$, then U and V have q^α common neighbors and no common neighbor if $\nu(b - d) = \alpha$ and $\nu(a - c) < \alpha$. Let A be the adjacency matrix of $\mathcal{SS}_{\mathcal{R}}$. For any two vertices U, V then $(A^2)_{U,V}$ is the number of common vertices of U and V . It follows that

$$A^2 = J + (q^r - 1)I - \sum_{\alpha=0}^r E_\alpha + \sum_{\alpha=1}^{r-1} (q^\alpha - 1)F_\alpha, \quad (3.8)$$

where:

- J is the all-one matrix and I is the identity matrix.
- E_α is the adjacency matrix of the graph $B_{E,\alpha}$, where for any two vertices $U = (a, b)$ and $V = (c, d) \in V(\mathcal{SS}_{\mathcal{R}})$, (U, V) is an edge of $B_{E,\alpha}$ if and only if $\nu(b - d) = \alpha$ and $\nu(a - c) < \alpha$.
- F_α is the adjacency matrix of the graph $B_{F,\alpha}$, where for any two vertices $U = (a, b)$ and $V = (c, d) \in V(\mathcal{SS}_{\mathcal{R}})$, (U, V) is an edge of $B_{F,\alpha}$ if and only if $\nu(b - d) = \alpha$ and $\nu(a - c) \geq \alpha$.

For any $\alpha > 0$, we have $|(z^\alpha)| = q^{r-\alpha}$, thus $B_{E,\alpha}$ is a regular graph of valency less than $q^{2r-\alpha}$ and $B_{F,\alpha}$ is a regular graph of valency less than $q^{2(r-\alpha)}$. Since eigenvalues of a regular graph are bounded by its valency, all eigenvalues of E_α are at most $q^{2r-\alpha}$ and all eigenvalues of F_α are at most $q^{2(r-\alpha)}$. Note that E_0 is a zero matrix.

Since $\mathcal{SS}_{\mathcal{R}}$ is a q^r -regular graph, q^r is an eigenvalue of A with the all-one eigenvector $\mathbf{1}$. The graph $\mathcal{SS}_{\mathcal{R}}$ is connected therefore the eigenvalue q^r has multiplicity one. Since the graph $\mathcal{SS}_{\mathcal{R}}$ contains (many) triangles, it is not bipartite. Hence, for any other eigenvalue θ , $|\theta| < q^r$. Let \mathbf{v}_θ denote the corresponding eigenvector of θ . Note that $\mathbf{v}_\theta \in \mathbf{1}^\perp$, so $J\mathbf{v}_\theta = 0$. It follows from (3.8) that

$$(\theta^2 - q^r + 1)\mathbf{v}_\theta = \left(\sum_{\alpha=1}^r E_\alpha - \sum_{\alpha=1}^{r-1} (q^\alpha - 1)F_\alpha \right) \mathbf{v}_\theta.$$

Hence, \mathbf{v}_θ is also an eigenvalue of

$$\sum_{\alpha=1}^r E_\alpha - \sum_{\alpha=1}^{r-1} (q^\alpha - 1)F_\alpha.$$

Since absolute value of eigenvalues of sum of matrices are bounded by sum of largest absolute values of eigenvalues of summands. We have

$$\begin{aligned} \theta^2 &\leq q^r - 1 + \sum_{\alpha=1}^r q^{2r-\alpha} - \sum_{\alpha=1}^{r-1} (q^\alpha - 1)q^{2(r-\alpha)} \\ &< 2rq^{2r-1}. \end{aligned}$$

The lemma follows. □

4 Proof of Theorem 1.10

Proof of Theorem 1.10. Let N be the number of solutions of the equation

$$f - e = (c - d)^2, \quad (c, d, e, f) \in C \times D \times E \times F,$$

where $C = f(A) + g(B)^2, D = g(B)^2, E = g(B), F = f(A)^2 + g(B)$. Hence, N is bounded by the number of edges between $-E \times C$ and $F \times -D$ in the sum-square graph $\mathcal{SS}_{\mathcal{R}}$. On the other hand, there is an edge between any two vertices

$$(-g(b_2), f(a) + g(b_1)^2) \in -E \times C, \text{ and } (f(a)^2 + g(b_2), -g(b_1)^2) \in F \times -D.$$

Since $\mu(f) = m_1$ and $\mu(g) = m_2$, we have $N \geq |A||B|^2/(4m_1m_2^2)$. It follows from Lemma 3.1 and Lemma 3.3 that

$$N \leq \frac{|C||D||E||F|}{q^r} + \sqrt{2r}q^{(2r-1)/2}\sqrt{|C||D||E||F|}.$$

Thus

$$\frac{|A||B|^2}{4m_1m_2^2} \leq \frac{|C||F||B|^2}{q^r} + \sqrt{2r}q^{(2r-1)/2}\sqrt{|C||F||B|^2}.$$

Solving this inequality gives us

$$|C||F| \gtrsim \min \left\{ \frac{|A|^2|B|^2}{m_1^2m_2^4q^{2r-1}}, \frac{q^r|A|}{m_1m_2^2} \right\},$$

which completes the proof of theorem. \square

Proof of Corollary 1.11. Since $|A| \gtrsim q^{r-1/2}$, $|A \cap R^*| \gtrsim |A|$. Thus we can assume that A is a subset in \mathcal{R}^* . Therefore, the corollary follows immediately from Theorem 1.10 by taking $f(x) = x$ and $g(y) = y^2$. \square

5 Proofs of Theorem 1.12 and Theorem 1.14

Proof of Theorem 1.12. First we set

$$S = \{(zh(x), zg(x)^{-1}) : (x, z) \in A \times C\}, T = \{(yz, g(x)(h(x) + y)) : (x, y, z) \in A \times B \times C\}$$

Since g and h are arbitrary functions, S and T can be multi-sets. Let S_1 and T_1 be sets of distinct points in S and T , respectively. Then we have

$$|S_1| \leq |A||C|, |T_1| \leq \min \{|A||B||C|, |f(A, B)||B \cdot C|\}.$$

Given a quadruple $(u, v, w, t) \in (\mathcal{R}^*)^4$, we now count the number of solutions (x, y, z) to the following system

$$g(x)(h(x) + y) = u, \quad yz = v, \quad zg(x)^{-1} = w, \quad zh(x) = t.$$

This implies that

$$g(x)h(x) = \frac{t}{w} = \frac{ut}{v+t}.$$

Since $\mu(g \cdot h) = m$, there are at most m different values of x satisfying the equality $g(x)h(x) = t/w$, and y, z are determined uniquely in terms of x by the second and the fourth equations. Therefore, the number of edges between S_1 and T_1 in the sum-product graph $\mathcal{SP}_{\mathcal{R}}(0)$ is at least $|A||B||C|/m$. On the other hand, it follows from Lemma 3.1 and Lemma 3.2 that

$$\frac{|A||B||C|}{m} \leq e(S_1, T_1) \leq \frac{|S_1||T_1|}{q^r} + \sqrt{2r}q^{(2r-1)/2} \sqrt{|S_1||T_1|}.$$

Solving this inequality gives us

$$|S_1||T_1| \gtrsim \min \left\{ \frac{q^r |A||B||C|}{m}, \frac{(|A||B||C|)^2}{m^2 q^{2r-1}} \right\}.$$

Thus, we obtain

$$|f(A, B)||B \cdot C| \gtrsim \min \left\{ \frac{q^r |B|}{m}, \frac{|A||B|^2|C|}{m^2 q^{2r-1}} \right\},$$

which concludes the proof of theorem. \square

Proof of Theorem 1.14. The proof of Theorem 1.14 is as similar as the proof of Theorem 1.12 by setting

$$S = \{(y + z, g(x)(h(x) + y)) : (x, y, z) \in A \times B \times C\},$$

$$T = \{(h(x) - z, g(x)^{-1}) : (x, y, z) \in A \times B \times C\}.$$

\square

6 Proofs of Theorem 1.16 and Theorem 1.17

Proof of Theorem 1.16. Let

$$S = \left\{ \left(yz, \frac{g(x)h(y)(x+y)}{h(yz)} \right) : (x, y, z) \in A \times B \times C \right\},$$

$$T = \left\{ \left(xz, \frac{zg(xz)h(yz)g(x)^{-1}h(y)^{-1}}{g(xz)} \right) : (x, y, z) \in A \times B \times C \right\}.$$

Then S and T are two sets of vertices in the sum-product graph $\mathcal{SP}_{\mathcal{R}}(0)$, and $|S| \lesssim |f(A, B)||B \cdot C|$, $|T| \lesssim |C||A \cdot C|$. Given a quadruple (u, v, w, t) in $(\mathcal{R}^*)^4$, we now count the number of solutions (x, y, z) to the following system

$$\frac{g(x)h(y)(x+y)}{h(yz)} = u, \quad yz = v, \quad \frac{zg(xz)h(yz)g(x)^{-1}h(y)^{-1}}{g(xz)} = t, \quad zx = w.$$

This implies that

$$xg(x)h(vx/w) = \frac{uw}{w+v}h(v). \quad (6.1)$$

Since $\max_u \mu(g \cdot h_u \cdot id) = O(1)$, there are at most $O(1)$ values of x satisfying the equation (6.1), and y, z are determined uniquely in terms of x by the second and the fourth equations. Thus, the number of edges between S and T in $\mathcal{SP}_{\mathcal{R}}(0)$ is at least $\gtrsim |A||B||C|$. The rest of the proof is the same as the proof of Theorem 1.12. \square

Proof of Theorem 1.17. First we set

$$S = \left\{ \left(yz, \frac{xy(g(x) + y)}{yz} \right) : (x, y, z) \in A \times B \times C \right\}, T = \left\{ \left(zg(x), \frac{z^2}{x} \right) : (x, z) \in A \times C \right\}.$$

Then S and T are two sets of vertices in the sum-product graph $\mathcal{SP}_{\mathcal{R}}(0)$, and $|S| \leq |f(A, B)||B \cdot C|$, $|T| \leq |A||C|$. We note that S and T can be multi-sets. Let S_1, T_1 be sets of distinct points in S and T , respectively. It follows from Lemma 3.1 and Lemma 3.2 that

$$e(S_1, T_1) \leq \frac{|S_1||T_1|}{q^r} + \sqrt{2r}q^{(2r-1)/2} \sqrt{|S_1||T_1|}. \quad (6.2)$$

On the other hand, given a quadruple (u, v, w, t) in $(\mathcal{R}^*)^4$, we now count the number of solutions (x, y, z) to the following system

$$\frac{xy(g(x) + y)}{yz} = u, \quad yz = v, \quad \frac{z^2}{x} = t, \quad zg(x) = w.$$

This implies that $g(x)^2x = w^2/t$. Since $\mu(g^2 \cdot id) = O(1)$, there are at most $O(1)$ values of x satisfying the equality $g(x)^2x = w^2/t$, and y, z are determined uniquely in terms of x by the second and the fourth equations. Therefore, we have

$$e(S_1, T_1) \gtrsim |A||B||C|. \quad (6.3)$$

Putting (6.2) and (6.3) together, we get

$$|A||B||C| \lesssim \frac{|S_1||T_1|}{q^r} + \sqrt{2r}q^{(2r-1)/2} \sqrt{|S_1||T_1|}.$$

This implies that

$$|S_1||T_1| \gtrsim \min \left\{ q^r |A||B||C|, \frac{(|A||B||C|)^2}{q^{2r-1}} \right\}.$$

Therefore,

$$|f(A, B)||B \cdot C| \gtrsim \min \left\{ q^r |B|, \frac{|A||B|^2|C|}{q^{2r-1}} \right\},$$

and the theorem follows. \square

References

- [1] N. Alon and J. H. Spencer, *The probabilistic method*, 2nd ed., Willey-Interscience, 2000.
- [2] M.F. Atiyah, I.G. Macdonald, *Introduction to commutative algebra* (Vol. 2). Reading: Addison-Wesley.(1969)
- [3] J. Bourgain, N. Katz, T. Tao, *A sum-product estimate in finite fields, and applications*, Geom. Funct. Anal. **14** (2004), 27–57.
- [4] J. Bourgain, *More on the sum-product phenomenon in prime fields and its applications*, International Journal of Number Theory, **1**(01) (2005), 1–32.
- [5] J. Bourgain, M. Z. Garaev, *On a variant of sum-product estimates and explicit exponential sum bounds in prime fields*, Math. Proc. Cambridge Philos. Soc. **146** (2009), no. 1, 1–21.
- [6] B. Bukh, J. Tsimerman, *Sumproduct estimates for rational functions*, Proceedings of the London Mathematical Society, (2011)pdr018.
- [7] A. Brouwer and W. Haemers, *Spectra of Graphs*, Springer, New York, etc., 2012.
- [8] G. Bini, F. Flamini, *Finite commutative rings and their applications*, Kluwer International Series in Engineering and Computer Science 680, Kluwer Academic Publishers 2002.
- [9] J. Cilleruelo, *Combinatorial problems in finite fields and Sidon sets*, Combinatorica **32**(5) (2012), 497–511.
- [10] W. Fulton, *Algebraic curves: An introduction to algebraic geometry*, Notes written with the collaboration of Richard Weiss. Reprint of 1969 original. Advanced Book Classics. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, (1989).
- [11] M. Z. Garaev, *The sum-product estimate for large subsets of prime fields*, Proc. Amer. Math. Soc., **136**(2008), 2735–2739.
- [12] M. Garaev, C.-Y. Shen, *On the size of the set $A(A+1)$* , Math. Z. **263**(2009), no. 94.
- [13] A. A. Glibichuk, S. V. Konyagin, *Additive properties of product sets in prime fields order*, Additive combinatorics, 279286, CRM Proc. Lecture Notes, 43, Amer. Math. Soc., Providence, RI, (2007).
- [14] D. Hart, L. Li, C-Y. Shen, *Fourier analysis and expanding phenomena in finite fields*, Proceedings of the American Mathematical Society, **141**(2)(2013), 461–473.

- [15] D. Hart, A. Iosevich, J. Solymosi, *Sum-product estimates in finite fields via Kloosterman sums*, Int. Math. Res. Not. no. 5, (2007) Art. ID rnm007.
- [16] N. Hegyvári, F. Hennecart, *Explicit construction of extractors and expanders*, Acta Arith. **140**(2009), 233–249.
- [17] N. Hegyvári, F. Hennecart, *Conditional expanding bounds for two-variable functions over prime fields*, European J. Combin., **34**(2013), 1365–1382.
- [18] N. Hegyvári, *Some remarks on multilinear exponential sums with an application*, Journal of Number Theory, **132**(1) (2012), 94–102.
- [19] N. Hegyvári, F. Hennecart, *A structure result for bricks in Heisenberg groups*, Journal of Number Theory, **133**(9) (2013), 2999–3006.
- [20] D. D. Hieu, L. A. Vinh, *On two-variable expanders over finite rings*, submitted. (2015)
- [21] N. H. Katz, C-Y. Shen, *A slight improvement to Garaev’s sum product estimate*, Proc. Amer. Math. Soc. **136** (2008), 2499–2504.
- [22] B. Nica, *Unimodular graphs and Eisenstein sums*, arXiv: 1505.05034 (2015).
- [23] L. Li, *Slightly improved sum-product estimates in fields of prime order*, Acta Arith. **147** (2011),no. 2, 153–160.
- [24] J. Solymosi, *Incidences and the Spectra of Graphs*, Building Bridges between Mathematics and Computer Science. Vol. **19**. Ed. Martin Groetschel and Gyula Katona. Series: Bolyai Society Mathematical Studies. Springer (2008), 499 – 513.
- [25] T. Tao, *Expanding polynomials over finite fields of large characteristic, and a regularity lemma for definable sets*, arXiv:1211.2894.
- [26] L.A.Vinh, *A Szemerédi–Trotter type theorem and sum-product estimate over finite fields*, European J. Combin., **32**(2011), no. 8, 1177–1181.
- [27] L.A.Vinh, *Product graphs, Sum-product graphs and sum-product estimate over finite rings*, *Forum Mathematicum*, Volume 27, Issue 3 (2015), 1639–1655.
- [28] H. V. Vu, *Sum-product estimates via directed expanders*, Mathematical research letters, **15**(2) (2008), 375–388.